IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF PUERTO RICO

UNITED STATES OF AMERICA, v. [1] WANDA VÁZQUEZ GARCED, [2] JULIO M. HERRERA VELUTINI, [3] MARK T. ROSSINI, Defendants.	CRIMINAL NO. 22-342 (SCC)

PROTECTIVE ORDER
PERTAINING TO CLASSIFIED INFORMATION

This matter comes before the Court upon the United States' *Motion for Protective Order Pursuant To Section 3 of the Classified Information Procedures Act* ("CIPA"). Pursuant to the authority granted under Section 3 of CIPA, the "Revised Security Procedures Established Pursuant to Pub. L. 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information" ("Security Procedures") (reprinted after CIPA § 9), Rules 16(d)(1) and 57(b) of the Federal Rules of Criminal Procedure, and the general supervisory powers of the Court, and to protect the national security, the following Protective Order is entered:[1]

1. The Court finds that this case will involve information that has been classified in the interest of national security. The storage, handling, and control of this information will require special security precautions mandated by statute, executive order, and regulation, and access to this information requires appropriate security clearances and need-to-know, as set forth in

[1] The Court understands that the government may move for a supplemental protective order depending on the nature of additional information that is determined to be discoverable.

Executive Order 13526 (or successor order), that has been validated by the government.[2] The purpose of this Order is to establish procedures that must be followed by counsel and the parties in this case. These procedures will apply to all pretrial, trial, post-trial, and appellate matters concerning classified information either disclosed by the United States to any defendant in this case or that any defendant reasonably expects to disclose or to cause the disclosure of in any manner in connection with any trial or pretrial proceeding in this case ("all classified information" or "all classified documents"). These procedures may be modified from time to time by further Order of the Court acting under its inherent supervisory authority to ensure a fair and expeditious trial.

2. Definitions. The following definitions shall apply to this Order:

a. "Government" or "the government" refers collectively to the Department of Justice prosecutors and support staff, as well as any law enforcement or intelligence community employees assisting in the prosecution of this matter.

b. "Defense" or "defense team" refers collectively to the respective counsel for Defendant Wanda Vazquez Garced, for Defendant Julio M. Herrera Velutini, and for Defendant Mark T. Rossini (the "Defendants"), and any support staff and consultants assisting the Defendants' respective counsel authorized to receive classified information pursuant to this Order.

~~c.~~ "Classified information" shall include any document, recording, or information that has been classified by any Executive Branch agency in the interests of national security pursuant to Executive Order 13526, as amended, or its predecessor or successor orders,

[2] Any individual to whom classified information is disclosed pursuant to this Order shall not disclose such information to another individual unless the CISO has validated that the proposed recipient possesses an appropriate security clearance and need-to-know.

as "CONFIDENTIAL," "SECRET," "TOP SECRET," or additionally controlled as "SENSITIVE COMPARTMENTED INFORMATION" ("SCI");.

d. "Document," "materials," and "information" shall include, but are not limited to:

i. all written, printed, visual, digital, electronic, or audible matter of any kind, formal or informal, including originals, conforming copies, and non-conforming copies (whether different from the original by reason of notation made on such copies or otherwise), as well as metadata;

ii. notes (handwritten, oral, or electronic); papers; letters; correspondence; memoranda; reports; summaries; photographs; maps; charts; graphs; inter-office communications; notations of any sort concerning conversations, meetings or other communications; bulletins; teletypes; telecopies; telegrams; telexes; transcripts; cables; facsimiles; invoices; worksheets and drafts; microfiche; microfilm; videotapes; sound recordings of any kind; motion pictures; electronic, mechanical or electric records of any kind, including but not limited to tapes, cassettes, disks, recordings, films, typewriter ribbons, word processing or other computer tapes, disks, or thumb drives and all manner of electronic data processing storage; and alterations, modifications, changes and amendments of any kind to the foregoing; and

iii. information obtained orally.

e. "Access to classified information" shall mean having access to, reviewing, reading, learning, or otherwise coming to know in any manner classified information.

f. "Secure Area" shall mean a Secure Working Area ("SWA") or Sensitive Compartmented Information Facility ("SCIF") approved by a designated Classified Information Security Officer ("CISO") for the appropriate storage, handling, and control of the classified

information in this case.

Classified Information

3. All classified documents, and classified information contained therein, shall remain classified unless the documents bear a clear indication that they are not classified or have been declassified by the agency or department that originated the document or information contained therein ("originating agency").

4. Access to classified information disclosed by the government or to be submitted to the Court as part of proceedings in this case shall conform to this.

5. The government may disclose classified information to the defense and/or the Defendants. The Defendants may also disclose classified information to the defense in a Secure Area. The Defendants or the defense may also disclose classified information to the government in a Secure Area. Any classified information provided to the defense by the government or the Defendants is to be used solely by the defense and solely for the purpose of preparing the defense. The defense may not disclose or cause to be disclosed in connection with this case any information known or reasonably believed to be classified information except as otherwise provided herein.

6. The defense may not disclose classified information to the Defendants unless that same information has been previously disclosed to the defense by the Defendants or unless the government has approved its release to the Defendants and marked it "Provided to Defendant/s [NAME], in *United States v. Wanda Vazquez Garced et al.*, 22-cr-342 (SCC)." Any classified information that the government discloses to the defense that is not to be shared with the Defendants shall be marked accordingly (for example, "Attorney's Eyes Only"). The defense may not confirm or deny to the Defendants the assertions made by the Defendants based on knowledge the defense may have obtained from classified information, except where that classified information has been provided to the Defendants pursuant to this Order. Any classified

information the defense discloses to or discusses with the Defendants shall be handled in accordance with this Order, including such requirements as confining all discussions, documents, and materials to an accredited Secure Area.

7. The defense and the Defendants shall not disclose classified information to any person, except to the Court, government personnel who hold appropriate security clearances and have been determined to have a need-to-know that information, and those specifically authorized to access that information pursuant to this Order.

8. Information that is classified that also appears in the public domain is not thereby automatically declassified unless it appears in the public domain as the result of an official statement by a U.S. Government Executive Branch official who is authorized to declassify the information. Individuals who, by virtue of this Order or any other court order, are granted access to classified information may not confirm or deny classified information that appears in the public domain. Prior to any attempt by the defense to have such information confirmed or denied at trial or in any public proceeding in this case, the defense must comply with the notification requirements of Section 5 of CIPA and all provisions of this Order.

9. In the event that classified information enters the public domain, the defense is precluded from making private or public statements where the statements would reveal personal knowledge from non-public sources regarding the classified status of the information, or would disclose that the defense had personal access to classified information confirming, contradicting, or otherwise relating to the information already in the public domain. If there is any question as to whether information is classified, the defense must handle that information as though it is classified unless the CISO confirms that it is not classified.

Security Procedures

10. In accordance with the provisions of CIPA and the Security Procedures, the Court has designated Daniella M. Medel as the CISO and Jennifer H. Campbell, Daniel O. Hartenstine, Matthew W. Mullery, Harry J. Rucker, and W. "Scooter" Slade, as alternate CISOs for this case, for the purpose of providing security arrangements necessary to protect against unauthorized disclosure of any classified information that has been made available to the defense in connection with this case. The CISOs listed above have the appropriate level of security clearances and need-to-know to handle classified documents in this case. The defense shall seek guidance from the CISO with regard to appropriate storage, handling, transmittal, and use of classified information.

11. The government has advised the Court that U.S. Department of Justice Public Integrity Trial Attorneys Nicholas Cannon and Ryan Crosswell, Assistant U.S. Attorney Seth Erbe, and U.S. Department of Justice National Security Division Trial Attorney Menno Goedman, as well as their supervisors ("counsel for the government"), have security clearances allowing them to have access to classified information that counsel for the government intend to use, review, or disclose in this case.

12. The Court has been advised, that counsel for the Defendants will coordinate with the CISO, to apply for and/or confirm the requisite security clearances. The CISO has been advised that the following members of the defense teams will apply through the CISO for a security clearance:

a. Defense team for Defendant Julio M. Herrera Velutini:

Lilly Ann Sanchez[3]

b. Defense team for Defendant Mark T. Rossini:

[3] The Government is aware that Defendant Julio Herrera may wish to add counsel for the purposes of this CIPA litigation. It is the Government's position that any attorneys intending to join the defense team for this litigation should be required to first file a notice of appearance with the Court.

Michael Nadler Juan Michelen

c. Defense team for Defendant Wanda Vazquez Garced: Ignacio Fernandez de Lahongrais

13. The CISO will work with the parties to ensure that the Defendant's counsel receive any requisite additional clearances prior to review of any information for which additional programs are applicable, should such a need arise.

14. *Protection of Classified Information*. The Court finds that to protect the classified information involved in this case, to the extent that defense counsel have the requisite security clearances and a "need-to-know" the classified information, they shall be given authorized access to classified national security documents and information as required by the government's discovery obligations and/or via their representation of the Defendants, and that their access to the same is subject to the terms of this Protective Order, the requirements of CIPA, and any other Orders of this Court.

15. To ensure the security procedures employed in this case are appropriate for the classification level of the classified information in this case, and to facilitate the filing of notices required under Section 5 of CIPA, the CISO shall make arrangements with the appropriate agencies to determine the classification level, if any, of materials or information either within the possession of the defense or the Defendants or about which the defense or the Defendants have knowledge and which the defense intends to use in any way at any pretrial proceeding, deposition, trial or post-trial or other proceeding. Nothing submitted by the defense to the CISO pursuant to this paragraph shall be made available to counsel for the Government or any law enforcement or intelligence community employees assisting in the prosecution of this matter unless so ordered by the Court or so designated by the defense.

16. To the extent the Defendants have previously entered into and executed agreements with the government, nothing in this order will terminate any continuing contractual obligations owed to the United States government, including any contractual obligations to not disclose to any unauthorized person classified information in the defendant's possession and/or classified information otherwise known to the defendant. Defendants will remain subject to this Court's authority, contempt powers, and other authorities, and shall fully comply with this Order.

17. Pursuant to Section 4 of the security procedures promulgated pursuant to CIPA, no court personnel required by this Court for its assistance shall have access to classified information involved in this case unless that person shall first have received the necessary security clearance as determined by the CISO.

18. Any additional persons whose assistance the defense reasonably requires may only have access to classified information in this case with the prior approval of the Court, if they are granted an appropriate security clearance through the CISO, and upon satisfying all the requirements in this Order for members of the defense team to have access to classified information. Counsel for the government shall be given notice of the individual to be added and given an opportunity to be heard in response to any defense request under this paragraph. If the Court approves the defense request, the CISO shall promptly seek to obtain the appropriate security clearances for the approved additional person or persons.

19. An individual with a security clearance and a need-to-know as determined by any government entity is not automatically authorized to disclose any classified information to any other individual, even if that other individual also has a security clearance. Rather, any individual who receives classified information may only disclose that information to an individual who has been determined by an appropriate government entity to have both the required security clearance

and a need-to-know the information.

21. *Secure Area for the Defense*. The Court is informed that the CISO will arrange for a Secure Area for use by the defense. The CISO shall establish procedures to assure the Secure Area is accessible during business hours to the defense, and at other times upon reasonable request as approved by the CISO in consultation with the United States Marshals Service. The Secure Area shall contain a separate working area for the defense and will be outfitted with any secure office equipment requested by the defense that is reasonable and necessary to the preparation of the defense. The CISO, in consultation with counsel for the Defendants, shall establish procedures to assure that the Secure Area may be maintained and operated in the most efficient manner consistent with the protection of classified information and in compliance with accreditation requirements. No classified documents, material, recordings, or other information may be removed from the Secure Area unless so authorized by the CISO. The CISO shall not reveal to the government the content of any conversations she/he may hear among the defense, nor reveal the nature of the documents being reviewed, or the work being generated. The presence of the CISO shall not operate to render inapplicable the attorney-client privilege.

20. *Filing of Papers by the Defense*. Any pleading or other document filed by the defense that counsel for the Defendants knows or reasonably should know contains classified information as defined in paragraph 2(c), shall be filed as follows:

a. The document shall be filed under seal as part of the classified record through the CISO or an appropriately cleared designee and shall be marked, "Filed in Camera with the Classified Information Security Officer." The time of physical submission to the CISO or an appropriately cleared designee shall be considered the date and time of filing and should occur no later than 4:00 p.m. Within a reasonable time after making a submission to the CISO, the defense

shall file on the public record in the CM/ECF system a "Notice of Filing" notifying the Court that the submission was made to the CISO. The notice should contain only the case caption and an unclassified title of the filing.

b. The CISO, or an appropriately cleared designee, shall immediately deliver to the Court and counsel for the government any pleading or document to be filed by the defense that contains classified information, unless the pleading or document is an *ex parte* filing.

21. *Filing of Papers by the Government*. Any pleading or other document filed by the government that counsel for the government knows or reasonably should know contains classified information as defined in paragraph 2(c), shall be filed as follows:

a. The document shall be filed as part of the classified record through the CISO or an appropriately cleared designee and shall be marked, "Filed in Camera with the Classified Information Security Officer." The time of physical submission to the CISO or an appropriately cleared designee shall be considered the date and time of filing and should occur no later than 4:00

p.m. Within a reasonable time after making a submission to the CISO, counsel for the government shall file on the public record in the CM/ECF system a "Notice of Filing" notifying the Court that the submission was made to the CISO. The notice should contain only the case caption and an unclassified title of the filing.

b. The CISO shall ensure the document is marked with the appropriate classification marking and remains under seal. The CISO, or an appropriately cleared designee, shall immediately deliver under seal to the Court and counsel for the defense any pleading or document to be filed by the government that contains classified information, unless the pleading or document is an *ex parte* filing.

22. *Record and Maintenance of Classified Filings*. The CISO shall maintain a separate sealed record for those materials which are classified. The CISO shall be responsible for maintaining the secured records for purposes of later proceedings or appeal.

23. *The Classified Information Procedures Act*. Procedures for public disclosure of classified information in this case shall be those established by CIPA. The defense shall comply with the requirements of CIPA Section 5 prior to any disclosure of classified information during any proceeding in this case. As set forth in Section 5, the defense shall not disclose any information known or believed to be classified in connection with any proceeding until notice has been given to counsel for the government and until the government has been afforded a reasonable opportunity to seek a determination pursuant to the procedures set forth in CIPA Section 6, and until the time for the government to appeal any adverse determination under CIPA Section 7 has expired or any appeal under Section 7 by the government is decided. Pretrial conferences involving classified information shall be conducted *in camera* in the interest of the national security, be attended only by persons granted access to classified information and a need-to-know, and the transcripts of such proceedings shall be maintained under seal.

24. *Access to Classified Information*. In the interest of the national security, representatives of the defense granted access to classified information shall have access to classified information only as follows:

a. All classified information produced by the government to counsel for the Defendants in discovery or otherwise, and all classified information possessed, created or maintained by the defense, including notes and any other work product, shall be stored, maintained and used only in the Secure Area established by the CISO, unless otherwise authorized by the CISO.

b. *Special procedures for audio and video recordings.* Any classified audio or video recordings that the government discloses to the defense shall be maintained by the CISO in the Secure Area. Such recordings may only be reviewed on a stand-alone, non-networked computer or other device within the Secure Area that does not have the capability to duplicate or transmit information. The defense must use headphones to review such recordings and the headphones must be wired and not have any wireless capability.

c. The defense shall have free access to the classified information made available to them in the Secure Area established by the CISO and shall be allowed to take notes and prepare documents with respect to those materials.

d. No representative of the defense (including, but not limited to, counsel, investigators, paralegals, translators, experts, and witnesses) shall copy or reproduce any classified information in any manner or form, except with the approval of the CISO and in accordance with the procedures established by the CISO for the operation of the Secure Area.

e. All documents prepared by the defense (including, without limitation, pleadings or other documents intended for filing with the Court) that do or may contain classified information must be prepared in the Secure Area on word processing equipment approved by the CISO. All such documents and any associated materials (such as notes, drafts, copies, typewriter ribbons, magnetic recordings, exhibits, thumb drives, discs, CDs, DVDs exhibits, and electronic or digital copies) that may contain classified information shall be maintained in the Secure Area unless and until the CISO determines those documents or associated materials are unclassified in their entirety. None of these materials shall be disclosed to counsel for the government or any other party.

f. The defense shall discuss classified information only within the Secure Area or in

an area authorized by the CISO.

g. The defense shall not disclose, without prior approval of the Court, classified information to any person not named in this Order except to the Court, Court personnel, and government personnel identified by the CISO as having the appropriate clearances and the need-to-know. Counsel for the government shall be given an opportunity to be heard in response to any defense request for disclosure to a person not identified in this Order. Any member of a Defense Team approved by this Court for access to classified information under this paragraph shall be required to obtain the appropriate security clearance, and to comply with all the terms and conditions of the Order. If preparation of the defense requires that classified information be disclosed to persons not named in this Order and the requirements of paragraph 19 have otherwise been met, the CISO shall promptly seek to obtain security clearances for them at the request of defense counsel.

h. The defense shall not discuss classified information over any standard commercial telephone instrument or office intercommunication systems, including but not limited to the Internet and electronic mail ("email"), or in the presence of any person who has not been granted access to classified information by the Court.

i. Any documents written by the defense that do or may contain classified information shall be transcribed, recorded, typed, duplicated, copied, or otherwise prepared only by persons who have received an appropriate approval for access to classified information.

j. The defense shall not disclose classified information to the Defendants unless that same information has been previously disclosed to the defense by the Defendants or unless the government has approved its release to the Defendants by marking it "Provided to Defendant/s [NAME], in *United States v. Wanda Vazquez Garced et al.*, 22-cr-342 (SCC)," absent written

permission of the government. Such permitted disclosure of classified information to the Defendant, as noted above, shall only be discussed by the defense within the Secure Area or in an area authorized by the CISO.

25. Any unauthorized disclosure or mishandling of classified information may constitute violations of federal criminal law. In addition, any violation of the terms of this Order shall be brought immediately to the attention of the Court and may result in a charge of contempt of Court and possible referral for criminal prosecution. Any breach of this Order may also result in termination of an individual's access to classified information. Persons subject to this Order are advised that direct or indirect unauthorized disclosure, retention or handling of classified documents or information could cause serious damage, and in some cases exceptionally grave damage to the national security of the United States, or may be used to the advantage of a foreign nation against the interests of the United States. The purpose of this Order is to ensure that those authorized to receive classified information in connection with this case will never divulge that information to anyone not authorized to receive it.

26. All classified documents and information to which the defense has access in this case are now and will remain the property of the United States. Upon demand of the CISO, all persons shall return to the CISO all classified information in their possession obtained through discovery from the government in this case, or for which they are responsible because of access to classified information. The notes, summaries, and other documents prepared by the defense that do or may contain classified information shall remain at all times in the custody of the CISO for the duration of the case. At the conclusion of this case, including any appeals or ancillary proceedings thereto, all such notes, summaries, and other documents are to be destroyed by the CISO in the presence of counsel for the Defendants if they choose to be present.

27. A copy of this Order shall be issued forthwith to counsel for the Defendants who shall be responsible for advising the Defendants and representatives of the defense of the contents of this Order.

28. Nothing contained in this Order shall be construed as a waiver of any right of the Defendant. No admission made by the Defendant or his counsel during pretrial conferences may be used against the Defendant unless it is in writing and signed by the Defendant. *See* CIPA § 2.

IT IS SO ORDERED.

Dated this _____ day of July, 2024.

HON. SILVIA L. CARRENO-COLL
UNITED STATES DISTRICT JUDGE